

大数据背景下计算机网络安全问题分析

林丙梅

(天府新区航空旅游职业学院 四川 成都 61113)

[摘要] 随着信息技术的飞速发展,二十一世纪已经进入信息化时代,计算机技术的广泛应用和普及对于社会生产力和经济水平的提高也发挥了至关重要的作用,给社会大众的日常生活带来了极大的便利。但与此同时,生活在大数据化、信息网络化的社会中,由于尚存在一定的技术漏洞,缺少相应的规范等原因,使得计算机网络安全性和隐私性也成为当前大数据背景下的计算机行业工作者面临的一大业务难关,针对这一现状,笔者对大数据背景下的计算机网络安全问题及应对措施进行深入探究,提出自己的观点,以供参考。

[关键词] 大数据背景;计算机技术;网络安全;现状

在信息化时代快速发展的阶段,基于信息资源大数据化的发展趋势,使得计算机网络信息普遍存在超大容量,传播迅速等特点,这一特点有利也有弊,有利之处在于通过计算机技术和网络信息大数据化,可以让社会大众快速搜索和接受到所需要信息,提高工作和学习效率,但弊处在于,恰恰因为信息的公开性和共享性,往往导致一些不法之徒利用技术漏洞实施不法行为,加之我国当前对信息行业的立法尚不完善,进而让其钻了法律的空子,造成行业内部的混乱,不利于信息技术行业的持续性发展。因此,如何有效的发现和解决大数据背景下计算机网络安全问题迫在眉睫。

一、大数据背景下的计算机网络安全现状

(一) 网络病毒种类繁多,难以控制

大数据时代的到来标志着计算机网络技术的进一步提高和普及,基于网络信息的便捷性和实用性,计算机在大众的日常生活和生活中已经必不可少,人们对网络的依赖程度也越来越高。虽然计算机信息技术一直在不断的更新和发展,但是由于网络病毒的种类和数量也随之增加,再加上网络信息传播的快速性,会在短时间内使得病毒对整个计算机系统的侵入程度扩大,有些病毒的危害性十分强大,可能会导致大量关键性数据和信息的丢失,给工作和生活造成难以挽回的损失。更有甚者,不法分子通过对计算机植入病毒进而远程操控电脑进行不法活动,严重的还可能造成社会秩序的混乱,扰乱社会经济的有序发展。

(二) 黑客技术发展迅猛,法律规范不够健全

信息资源大数据化已经成为当前全世界范围内的大趋势,计算机信息专业的人才数量越来越多,这也催生出了计算机黑客这一潜在行业的产生和发展。黑客利用自身高超的计算机操作能力,有目的,有针对性的执行相应的破坏任务,采取形式多样也极具隐蔽性的攻击手段逃避正常的监督,对受侵害电脑系统的程序和硬件造成破坏。除此之外,我国在计算机信息行业领域内的法律规范尚不够完善,相应的法律法规等强制性手段的建立也尚处于初步探索阶段,从而造成一系列法律漏洞,具体到黑客这一灰色产业来说,更是由于没有法律对其进行规制而变得愈发猖狂,对于整个计算机信息领域的安全造成巨大隐患。

(三) 盗版系统猖狂,计算机硬件设施不过关

对于计算机网络安全来说,不仅要注重系统内部的维护和监督,更要同时确保硬件设施的安全,硬件设施的达标会有效的降低计算机所遭受的威胁,提高自身的安全性。然而在实际生活中,有很大一部分的私人或单位的计算机在安装时为了减少资金投入,都选择安装盗版系统,这也为后期计算机系统内部的大数据信息的安全性保障带来了不利的影响,比如在这些盗版系统中可能会存在网络拓扑结构不合理、防火墙等安全设施不到位等问题,这些都会影响计算机网络安全。

(四) 计算机信息传播途径的安全问题

信息传播在计算机网络的发展过程中占据着至关重要的地位,因此,如果在信息传播过程中出现问题,那么极有可能造成整个工作流程的崩塌,给后续活动的开展带来巨大的打击。数据信息是以通信协议为前提传递的,例如,HTTP、TCP/IP等通讯协议,而这些协议随着计算机技术的迅猛发展已经不再能够完全应对现

在的网络漏洞,存在一定的缺陷,进而被一些不法信息窃贼者钻空子,导致大量数据的丢失。

二、解决大数据背景下计算机网络安全问题的可行性措施

(一) 行业工作人员要不断提高自身的专业技能

计算机信息技术的发展和革新速度是十分迅猛的,因此,要想保障计算机信息的安全性,工作人员就必须紧跟行业的发展步伐,及时的借鉴和学习前沿的理论更新,锻炼自己的操纵能力,提高自身的专业水准,从而在遇到问题时能够及时反应,有效应对。

(二) 防范网络病毒和黑客攻击

众所周知,计算机网络系统一旦被病毒入侵后往往很难解决,轻者重装系统,重者可能会对计算机造成永久性破坏。因此,加强对病毒的防范非常重要。众多防火墙的开发和杀毒软件的应用对于预防和阻绝电脑病毒的入侵有着积极的效果,因此,计算机信息技术领域的研发人员一定要注重对杀毒软件的及时更新和完善,不断修补系统漏洞,提高计算机网络的安全性。

其次,我国还应该加强对黑客产业的法律规制,制定相应的法律法规等强制性措施,规范和监督不法分子利用黑客技术和法律漏洞实施破坏计算机系统安全性的违法行为,从根源上约束和打击猖獗的黑客技术的实际应用,从而保护网络信息的安全。

(三) 修复计算机网络漏洞,对网络信息的安全进行全程跟踪

计算机技术更新换代极快,许多安全漏洞的出现往往使我们措手不及,因此,行业工作者不仅要注重源头预防,更要确保在出现安全问题进行及时修复,及时止损。及时修复漏洞会有效阻止病毒的进一步扩大和传播,最大程度上降低危害后果。此外,还要重视对网络信息安全传播的全程监督和保密,即可以开发专门性的软件,对网络信息进行安全加密,保障信息在传输过程中的安全性。

结束语:

总而言之,信息技术的迅速发展和广泛应用使得计算机网络已经成为我们日常生活中不可或缺的一部分,大量的网络信息资源给我们的学习和生活都带来了极大的便利,但是,我们也不能忽视,它在迅猛发展的过程中也伴随着众多安全问题的产生。比较常见的如计算机病毒、黑客入侵等安全隐患,对于计算机网络的安全性带来了不利的影响,因此,不论是行业内部的专业人士还是私人使用者,都必须要加强对于计算机系统的安全性防护,保证网络信息的安全传输,确保计算机行业的有序运行和社会秩序的稳定。

参考文献:

- [1] 张传勇. 基于大数据时代下的网络安全问题分析[J]. 网络安全技术与应用, 2015(01).
- [2] 徐海军. 大数据时代计算机网络安全防范研究[J]. 计算机光盘软与应用, 2014(23).
- [3] 那伟宁. 大数据时代的计算机网络安全及防范措施[J]. 电子技术与软件工程, 2017, 10(23): 195-195.

林丙梅, 1986, 女, 四川省乐山市人, 本科, 学士, 天府新区航空旅游职业学院, 四川省成都市温江区, 611130